Available online at www.sciencedirect.com

ScienceDirect

Procedia Economics and Finance 15 (2014) 401 – 405

Procedia Economics and Finance

www.elsevier.com/locate/procedia

Emerging Markets Queries in Finance and Business

Principles of security and integrity of databases

Șerban Mariuța [a, *]

[a]*University of Pitești, Pitești, 1 Targul din Vale, Romania*

Abstract

To reduce the risk of loss and destruction of information stored in a database, the management of an organization should use the implementation of various security methods.
A comprehensive strategy to secure a database is more than data security. Usually, security events can be associated with the following action: illegal access to data confidentiality damage, damage to the integrity of data, loss of data availability. Loss of privacy of information, making them accessible to others without right of access is not visible in the database and does not require changes dedectabile database.
This paper addresses these events to ensure database security.

Selection and peer-review under responsibility of the Emerging Markets Queries in Finance and Business local organization

Keywords: security; authentication; authorization; access control;

1. Introduction

Database security concerns the use of a large spectrum of controls of information security to protect databases (this includes: data, database applications or stored functions, database systems, database servers and according links to the network) against breaking of confidentiality, integrity and availability. This involves different types of category controls such as: technical, procedural/administrative and physical. Database security is a special subject in the area of computers security, information security and risk management.

Regarding the level of security a differentiation is made, firstly between two separate levels of security, which are:

* Corresponding author. Tel.: +0 -0723 679214.
E-mail address: mariuta_serban@yahoo.com.

Selection and peer-review under responsibility of the Emerging Markets Queries in Finance and Business local organization
doi:10.1016/S2212-5671(14)00465-1

- Low security, representing the security which call for some guarantees against vulnerabilities which can be exploited by unintelligent opponents (such errors input by environment which can be corrected by redundant mechanisms such as error corrections codes);
- High security, call for some guarantees against vulnerabilities which can be exploited by intelligent opponents (such as human, intelligent software agents). High security is mainly ensured by encryption techniques, but not entirely, for example the viruses can be considered as intelligent agents who exploit systems but encryption does not offers viable solutions regarding this.

A security policy includes hardware and software security, data transitions security, physical security, documents and data sources security.

The role of security services is to monitor security attacks and stop the original not a copy.

- Authenticity supposes that two entities which are involved in a data exchange be able to identify one to another and to prevent another entity to steel their identity.
- Data integrity suppose the existence of this attacks.

Among security services are:

- Confidentiality which represents protection of data that are sent against the passive attacks. This security service is indispensable in banking services where the document is required, unchanging by an unauthorized person of the content.

- Non-repudiation which represents that every entity cannot deny an executed service, each entity assuming the responsibility of the messages. The receiver can prove that the received message is the authentic message sent by expeditor and not conversely. This security service is very important for electronic contracts. For example an order of a such value cannot be repudiated subsequently by any part claiming that initially another lower amount had been agreed.

- Data access control involves limiting the access of users to data. For fulfilling this service should identify and then the rights of access are verified.

- Availability of data involves that data is available only for authorised persons.

2. Security mechanisms

The security is a broad topic and covers many imperfections. Data security issues are often caused by various malicious people to obtain information, benefits and to cause harm.

The implementation of a security mechanism facilitates security services. The role of security is to detect and prevent a security attack.

The following security services are used for implementation of security services:

- Encryption represents data codification process, which can be accessed only by the user that owns the secret key for decoding. The role of data encrypting is to ensure the confidentiality of data. To ensure that the data comes from the authorized user, a digital signature is used, which can be obtained through the following two processes: data signing and data validation.
- Access mechanism implicates the control of user's access to resources, with each user being authorized and able to login to the requested resources. The process takes place when unauthorized access to a resource happens. The control policy as regards the access should contain at least the following elements:
  - A list with all the access rights;
  - Usernames and passwords;
  - Security labels;
  - How much time has the right to access the resource;
  - Length of time requires to entry in possession of the access;
  - Test access path.
- Data integrity mechanism refers to integrity of data, without being able to be modified, altered or removed

The integrity can be regarded from two ways in the following two ways:

- Traffic integrity , using cryptographic changing or time marking
- Entity's integrity, using BCC cryptographic checksum (Block Check Code).

- Authentication mechanism is used to authenticate the users, process achieving through a username and a password.
- Notice mechanism refers to the implication of another entity, known as notices, where all the entities involved fully trust it, and which ensures the originality, integrity and confidentiality of the information.

3. Validation of data integrity

In order to verify if there are errors in the database as regards integrity of data, procedure DBCC CHECKDB is used. It is recommended to run this procedure on each type of database, at certain period of time, because some errors are difficult to be discovered by the database server.

By implementing the maintenance database plan, the database administrator weekly verifies the possible errors. In case it is known that the system does not recognize and corrects the errors, the verification procedure DBCC CHECKDB is manually executed.

Database is blocked while DBCC CHECKDB procedure runs and this can constitute a disadvantage because checkings can last longer for large dimension databases.

The errors reported after running DBCC CHECKDB procedure should be corrected as soon as possible. That's why the option REPAIR_REBUILD of repairing the database with minimal losses is used. Using this option is not recommended because by repairing the lost data, different problems can occur, only if there is no backup before the corruption event.

SQL Virtual Restore allows creating a database efficient and fully functional by restoring a backup. This involves running stricter controls backup database from those possible without completely restore.

By using DBCC CHECKDB procedure the logical and physical integrity of all objects in the restored database is verified. A copy of a database restored and checked with option VERIFYONLY may have serious problems regarding data integrity.

Checking the integrity of data from a database can be done automatically or manually. These commands have the same effect and the same purpose when applied to a restored database from a copy of the data base and a database of standard.

Before running this procedure is recommended to close all applications (Business Services Manager Tivoli Systems).

The responsibilities of a DBA database administrator are usually reflected in phenomena such as performance optimization, capacity planning and disaster recovery. Ensuring the database integrity at both logical and physical level is omitted or deferred. No one can control how long the task will run. Even the Properties menu contains a variety of settings as regards the maintenance, but no details about how to run the DBCC procedures.

Wherever used the CHECKDB verification procedure is recommended the use of WITH NO_INFOMSGS option, option which suppresses all output of irrelevant data such as how many rows are in each table. If it is desired to know this type of information, this can be achieved by simple queries, but not when DBCC procedures are running. Suppressing these data make visible the existence of a critical message.

If running DBCC CHECKDB on SQL Server 2008 or SQL Server 2005, the option to always ALL_ERRORMSGS needs to be checked, because in these cases, the list of errors on object is truncated to 200. In Management Studio the error list resulted after run DBCC CHECKDB procedure is limited to 1000 lines, having the risk to lose some errors if the number of errors exceeds this figure. Therefore any operation other than a quick CHECKDB differs from ad-hoc verification, where the results should be directed in order to be stored in a file. This measure eliminates the resumption of proceedings if is not a measure strictly linked

performance and is considered to be particularly important if the verification occurs during the database recovery in case of disaster.

The syntax of DBCC CHECKDB procedure, together with all the possible option, is the following:

```
DBCC CHECKDB
( 'database_name'
    [ , NOINDEX
      | { REPAIR_ALLOW_DATA_LOSS
        | REPAIR_FAST
        | REPAIR_REBUILD
        } ]
) [ WITH { [ ALL_ERRORMSGS ]
    [ , [ NO_INFOMSGS ] ]
    [ , [ TABLOCK ] ]
    [ , [ ESTIMATEONLY ] ]
    [ , [ PHYSICAL_ONLY ] ]
    }
]
```

The "database_ name" argument is the name of the database for which the integrity is checked; if not specified, the procedure runs for the current database.

NOINDEX is useful because it reduces the execution time by specifying the indexes which should not be checked.

In order to repair errors revealed by BCC CHECKDB procedure one of the following options can be used:

- REPAIR_FAST realizes minor repair actions, such as the repair of supplementary keys of indices, by saving time. These repairs are realized fast, with no risk of losing the data.
- REPAIR_REBUILD Besides the repaired performed with REPAIR_FAST option, this option performs repairs which need time, such as reconstruction of the indices. These repairs are realized without the risk of losing the data.
- REPAIR_ALLOW_DATA_LOSS Realize all the repairs performed by REPAIR_REBUILD option, including the allocation/deallocation of the rows or pages to correct the allocation errors or page errors, also the erase of the corruption objects/texts. This type of repair can lead to the loose of data. The repair is made through a transaction which permits the user to return the previous stage of the changes performed.

The WITH option returns the number of error messages, the number of blocks occurred or the estimations of the tempdb requests. This can be performed through the following controls described in Table 1.

Table 1: Controls for option WITH

Controls for WITH	Description
ALL_ERRORMSGS	Gives an unlimited number of errors on object. If this number is not specified, than maximum 200 error messages run for each object.
NO_INFOMSGS	Eliminates all the informative messages and the reports of the space used.
TABLOCK	Gives the possibility to run the DBCC CHECKDB procedure faster, in a difficult database, but the competition decrease during the running time..
ESTIMATE ONLY	Gives the estimative value of tempdb space necessary to run the procedure CHECKDB with specific option, while the check does not take place.
PHYSICAL_ONLY	This control detects the broken pages or the hardware errors which can compromise an user data.

4. Conclusions

The security is a broad topic and covers many imperfections. Data security issues are often caused by various malicious people to obtain information, benefits and to cause harm.

Ensuring data security databases is achieved by following two rules:

- Security requirements, implying vulnerability management and review;
- Managing the access.

The DBCC CHECKDB procedure is used to check the errors in database regarding the data integrity. DBCC CHECKDB procedure is often undervalued by managers of a database; it represents a very important, often crucial aspect for protecting the business data.

Acknowledgements

Many sincere thanks to my supervisor, Prof. dr. Horia-Ioan Georgescu, who accepted me as PhD. Sudent and who guided me and offered me a great support in my research.

References

Barnes R.. Database Security and Auditing: Leading Practices. Enterprise Auditing Solutions Applications Security; 2011.

Băjenescu T.I..Progresele informaticii, criptografiei şi telecomunicaţiilor în secolul 20. Bucureşti. Editura Matrix Rom;2003.

Bertrand A, Mnimizing the impact of DBCC CHECKDB: Dos ahn Don'ts,november 29, 2012, http://www.sqlperformance.com/2012/11/io-subsystem/minimize-impact-of-checkdb.

Blue Coat, Top Five Security Best Practices for you Web Gateway în 2009, http://networking.ittoolbox.com/research/top-five-security-best-practices-for-your-web-gateway-in-2009-19108.

Fusaru D. Arhitectura bazelor de date. Mediul SQL, Editura Fundaţiei România de Mâine, Bucureşti. 2002.

Hicks J., Criptography in SQL Server. http://msdn.microsoft.com/enus/library/cc837966%28v=sql.100%29.aspx. 2008.

Lesov P. Database Security: A Historical Perspective. University of Minnesota. CS 8701; 2008.

Srikanth, Radhakrishna., Database security best practices. www.helium.com; 2011.

Şerban M., Protection and security of data base information. Annals of Spiru Hart University, Economic Series, Volumul 2(11); 2011, pag. 93-100, ISSN 2068-6900.

http://en.wikipedia.org/wiki/Database_security.

http://msdn.microsoft.com/en-us/library/aa258281(v=sql.80).aspx.